We claim:

1. In an authentication chip in which secret data is manipulated, a method of shielding manipulations of the secret data from observation, including the steps of:

operating non-flashing CMOS structures in the chip, in which pMOS and nMOS transistors are driven such that they do not have intermediate resistance simultaneously during a change of state of the CMOS structure, to manipulate the secret data; and

operating conventional CMOS inverters adjacent the non-flashing CMOS structures at the same time.

2. A method according to claim 1, including the further step of generating continuous circuit noise to drive the conventional CMOS inverters.

3. A method according to claim 2, including the further step of generating continuous circuit noise to a tamper detection line and driving the conventional CMOS structures from the tamper detection line.

4. A method according to claim 1, including the further step of driving the conventional CMOS multiple times faster than the non-flashing CMOS.

5. An authentication chip for performing the method, comprising:

non-flashing CMOS structures, in which pMOS and nMOS transistors are driven such that they do not have intermediate resistance simultaneously during a change of state of the CMOS structure, to manipulate the secret data; and

conventional CMOS inverters adjacent the non-flashing CMOS structures, to change state at the same time the non-flashing CMOS structures manipulate secret data.

6. An authentication chip according to claim 5, further including a noise generator connected to the conventional CMOS inverters to drive them with continuous circuit noise signals.

7. An authentication chip according to claim 6, further including a tamper detection line connected between the noise generator and the conventional CMOS structures.

8. An authentication chip according to claim 5, where the conventional CMOS is driven multiple times faster than the non-flashing CMOS.